Indian J. Phys. **44**, 232–243, (1970)

Generation and properties of multilevel pseudo-random sequences

By N. B. Chakraborti

Department of Electronics and Electrical Communication Engineering, Indian Institute of Technology, Kharagpur, West Bengal

and

A. K. Mukherjee

Institute of Radio Physics and Electronics, 92 Acharya Prafulla Chandra Road, Calcutta-9. West Bengal. (*Received 16 January 1970*)

In this paper generation and properties of multilevel sequences are discussed. The use of phase logic for generating RF multiphase-pseudo-random sequences is described Application of these codes in communication and schemes for ternary counting and binary-ternary conversion are presented.

Introduction

There has been considerable interest in recent years in binary quasi-random sequences with particular reference to their application in radar, communication systems and automatic error-correction circuits.

Pseudo-random sequence (prs) is so-called as it has some important characteristics in common with random noise. These are (*i*) a complicated looking structure which makes a part of the waveform indistinguishable from a sampled function of noise, (*ii*) nearly zero average value over a specified period, (*iii*) a sharp auto-correlation function.

But such sequences are better suited for application in that (*i*) they can be generated by a perfectly deterministic process, and (*ii*) the peak factor can be made much lower than that of random noise.

When the sequences are made of presence or absence of a pulse or the positive and negative pulse, or any other set of two distinct states then we call it a binary prs. In multilevel prs similarly, we must have larger number of states which may be pulses of different amplitude, sine or cosine functions with different phases or frequencies or any other recognizable parameters.

It has been suggested (Briggs 1966) that ternary prs can be generated by addition of a binary sequence with its transformed version. Sequences thus obtained are seen to have a spread out correlation function.

In the present paper, techniques of generation of multilevel sequences, which are based on shift-register techniques as employed for generating binary sequences, are described. The two state flip-flops are replaced by multistate devices. The

logic remains still modular but the moduli may be prime or non-prime and take on values of 3, 4, 5, etc. Multistate devices where states signify specified amplitudes are difficult to realize if the number of states exceeds 3. However, if the states are made to signify the phases of a carrier then multistate devices and logical units (*e.g.*, modular adder, multiplier) can quite easily be realized.

Generation of multilevel sequences both on amplitude and phase basis are considered in Section 1. Properties of such sequences are also discussed here Realization of such sequences both on amplitude and phase basis is discussed in Section 2. Application of such codes in communication and other special purposes and the advantages arising out of their use are discussed in Section 3.

Section 1

Multilevel Sequences and Their Properties

Multilevel sequences having n levels can be generated, using s-stage multilevel shift register (Taub 1968) with proper feedback (according to the generating polynomial) to the first stage, which is the modulo-n-sum (Pugh 1967) of the outputs of the appropriate stages multiplied by 1, 2, ... or n.

The maximum length which can be generated in an n-level generator is $L = n^s - 1$, where n is the number of levels in the sequence and s (determining the length) is the degree of the generating polynomial. The polynomial chosen must be irreducible. To find out the irreducible polynomials of a given degree one has only to eliminate the polynomials which can be factorized into polynomials of lower degree. The irreducible polynomials for prime modulo 3, 5 and 7 have been tabulated by Church (1935). It has to be mentioned that an irreducible generating polynomial does not necessarily lead to a maximal length sequence. In other words, the irreducible character is a necessary but not a sufficient condition for generating sequences of maximal length.

The polynomials of modulus-3 give rise to ternary sequences and the polynomials are listed by Elspas (1959). The sequences obtained with these polynomials are presented here in table 1.

To understand the operation of the generator one may consider for example, a ternary function $D^3 \underset{3}{\oplus} 2D^2 \underset{3}{\oplus} I = 0$ with the initial condition 012. Here one must keep in mind that addition and multiplication obey modular logic. With such an arrangement the multistate device will successively go through the states 012, 201, 220, 222, 022, 002, 100, 010, 101, 210, 121, 112, 211, 021, 102, 110, 111, 011, 001, 200, 020, 202, 120, 212, 221, 122, 012, ... Thus after 26 changes the shift registers have come back to the original 012 state and again the sequence is repeated. Thus at the output one will have a repetitive sequence given in the table below.

Table 1

generating polynomial	length	sequences obtained
1. $D^3 \underset{3}{\oplus} D^2 \underset{3}{\oplus} 2D \underset{3}{\oplus} 1$	26	01200221222010210011211102
2. $D^3 \underset{3}{\oplus} 2D \underset{3}{\oplus} 1$	26	01221202001110211210100222
3 $D^2 \underset{3}{\oplus} 2D^2 \underset{3}{\oplus} 1$	26	01211201110020212210222001
4. $D^3 \underset{3}{\oplus} 2D^2 \underset{3}{\oplus} D \underset{3}{\oplus} 1$	26	01222120101100211121020220
5. $2D^3 \underset{3}{\oplus} 2D^2 \underset{3}{\oplus} 1$	13	0121001011122, 0212002022211
6. $2D^3 \underset{3}{\oplus} D \underset{3}{\oplus} 1$	13	0121022111010, 0212011222020
7. $D^3 \underset{3}{\oplus} D^2 \underset{3}{\oplus} D \underset{3}{\oplus} 2$	13	0120022122201, 0210011211102
8. $2D^3 \underset{3}{\oplus} D^2 \underset{3}{\oplus} D \underset{3}{\oplus} 1$	13	0120201112110, 0210102221220

It is observed that after 13 bits the sequence is an exact repetition of the earlier bits with positions of 1 and 2 interchanged. In the last four polynomials the sequence repeats itself after 13 bits.

If the value of s is increased to 4, the length of the sequence corresponding to an irreducible generating polynomial may be 5, 10, 16, 20, 40 and 80, *i.e.*, there may be 16 sequences of length 5, 8 sequences of length 10, 5 sequences of length 16, 4 sequences of length 20, 2 sequences of length 40, or a single sequence of length 80. But if the polynomial chosen is reducible then we will have sequences of unequal length depending on the initial conditions of the registers.

When the sequences generated are not of maximal length *i.e.*, $L \neq n^s - 1$ all the possible permutations of the states do not occur. The length then obtained corresponds to a subset of the permutation and depends on the initial conditions The subsets are in general closed on themselves and mutually exclusive.

So far we were discussing the sequences derived from generating polynomials corresponding to prime modulus. But in case of sequences obtained from non-prime modulus such as 'quaternary' or 'sextic' sequences (*i.e.* the sequences which consist of 4 or 6 different states) even if one chooses the prime polynomial, the length obtained is not equal to $(n^s - 1)$, the sequence breaks up into several subsequences depending on the initial conditions.

Table 2 shows the quaternary sequences obtained corresponding to generating polynomials listed. The maximum length for polynomial of degree 3 is 14. There are 4 sequences of length 14 and a single sequence of length 7, totalling 63 possible states. The sum of the lengths of all the possible subsequences of a given generating polynomial is equal to n^s-1.

Table 2

generating polynomial	length	sequences obtained
$D^3 \underset{4}{\oplus} D \underset{4}{\oplus} I$	14	00131230231103,
		00313210213301,
		01221112120331,
		03223332320113,
	7	0022202
$D^3 \underset{4}{\oplus} 2D \underset{4}{\oplus} I$	14	01221310100333,
		03223130300111,
		02113212031121,
		02331232013323,
	7	0022202
$D^3 \underset{4}{\oplus} 3D^2 \underset{4}{\oplus} I$	14	01211302123112,
		03233102321332,
		00101312210333,
		00303132230111,
	7	0020222
$D^3 \underset{4}{\oplus} D^2 \underset{4}{\oplus} I$	14	01231300103312,
		03213100301132,
		01330212111221,
		03110232333223,
	7	0020222
$3D^3 \underset{4}{\oplus} D \underset{4}{\oplus} I$	14	01223330300313,
		03221110100131,
		01132302133212,
		03312102311232,
	7	0022202
$3D^3 \underset{4}{\oplus} 3D \underset{4}{\oplus} I$	14	01223132320311,
		03221312120133,
		00111230211301,
		00333210233103,
	7	0022202
$3D^3 \underset{4}{\oplus} D^2 \underset{4}{\oplus} I$	14	01233300301332,
		03211100103112,
		01130232313221,
		03310212131223,
	7	0020222
$3D^3 \underset{4}{\oplus} 3D^2 \underset{4}{\oplus} I$	14	01213302321132,
		03231102123312,
		00101112230131,
		00303332210313,
	7	0020222

An observation of the sequences shows that the 4 sequences of length 14 corresponding to a fixed polynomial consist of two pairs, a sequence in a pair being obtainable by interchanging the positions of one and three in the other.

Similarly the maximum length for polynomials of degree 4 is 30. Some of these are symmetric with 1 and 3 positions interchanged and others are asymmetric.

Properties

The first point to note is that the sequences have zero or nearly zero average value over a specified length. This is true in case of a prime modulus. This property follows from the fact that the length obtained is the permutation of all the possible sets of states excepting 000 ... 0, the different states occur equal numbers of times to enable the average value to be zero. But in case of non-prime modulo the sequences do not contain all such permutation and so the average value is in general not equal to zero.

The modulo sum of two members of such sequences gives rise to another sequence whether the sequences are generated corresponding to a polynomial of prime or non-prime modulus. The sequences thus obtained are the shifted version of the sequence or its conjugate (*i e.*, the same sequence with 1 or 2 position interchanged in case of ternary and 1 and 3 position interchanged in quaternary). This is in general true for any shift-register generated sequence.

Considering the aperiodic auto-correlations of the sequences of length 13, we see that the side-lobes are 1/8th of the peak. The periodic auto-correlations of such sequences are also found to be of the same character. The cross correlation properties of such sequences are found also to be very good. Unfortunately, however, the correlation properties of sequences of larger length are not that good. This is true for sequences generated corresponding to polynomial of non-prime modulo. They are good enough to be used in connection with correlation detection method. Thus generally, we can say that correlation properties of the multilevel prs's are same as that of binary prs's but the ternary sequences of length 13 have the unique properties of a correlation as described earlier and they may be classified as optimum correlation (Golomb & Scholtz, 1965) ternary prs's. This correlation output is shown in figure 1.

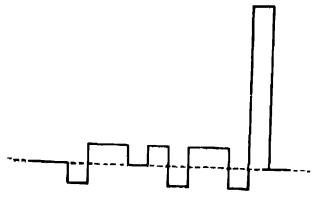

FIGURE 1. Digital matched filter output of a 13 bit ternary prs with digital delay.

The power spectrum of the multilevel prs is of the same nature as that of the binary prs. The minima will occur at a frequency equal to the multiple of the pulse repetition frequency (prf). The first maximum occurs at f/k, where f is the prf and k is the number of bit in the sequence. The other maxima occur at $\left(\frac{2k+1}{2}\right) f$ and $k = 1, 2, \ldots$.

Error Probabilities in Ternary Decoding

In ternary coding on amplitude basis the three states are 0, 1, and -1. The decision circuit will include a threshold element with a level of $|a|$. The output will be recognised as 1, if input exceeds a and -1 if the input is less than $-a$ and otherwise as zero (*i.e.*, it lies between $-a$ and $+a$). When a zero is sent an error would occur if $|n_c|$ is greater than a where n_c is the inphase component of noise. Similarly if 1 [or -1] is sent the error would occur if $(S+n_v) < a$ [or $(n_c - S) > -a$], where S is the signal component. If the *a priori* probabilities of the states are represented as $p(0)$, $p(1)$ and $p(-1)$ the error probability is

$$P_e = p(0)\, p_{e(0)} + p(1)\, p_{e(1)} + p(-1)\, p_{e(-1)}$$

where p_{eA} is the error probability when A is sent.

Now

$$p_{e(1)} = \frac{1}{\sqrt{2\pi}\sigma}\left[\int_{-\infty}^{0} e^{-x^2/2\sigma^2}\, dx - \int_{0}^{S-a} e^{-x^2/2\sigma^2}\, dx\right].$$

$$p_{e(-1)} = p_{e(1)}$$

$$p_{e(0)} = 1 - \frac{2}{\sqrt{2\pi}\sigma}\int_{0}^{a} e^{-x^2/2\sigma^2}\, dx.$$

In figure 2 the variation of error probability with SNR is plotted for different values of the relative threshold a/S.

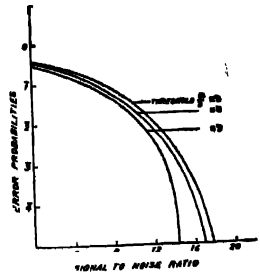

FIGURE 2. Error probabilities of ternary de-coding.

Section 2

Realization of Such Sequences

For generating a ternary sequence the same ideas as employed in the case of binary are used The block diagram of such a system is shown in figure 3. Here D represents the three level shift register element and $\underset{3}{\oplus}$ represents the mod3 adder. The multiplying units are represented by $\boxed{x1}$ or $\boxed{x2}$.

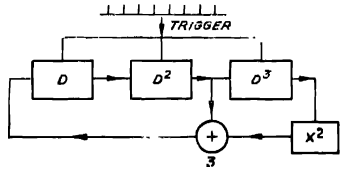

Figure 3. Block diagram of 3 level prs generator.

In the diagram the logic is set according to the generating polynomial $D^3 \underset{3}{\oplus} 2D^2 \underset{3}{\oplus} I = 0$ initial condition like 012, 121, 211, or any other permissible set is forced on the ternary shift register. The output of any of the shift register or the mod3 adder will give the specified sequence.

In general, sequences we require circuits with more than three stable states. These circuits are quite difficult to build and the multi-level logic circuits are not available. So one has to take resort to three or multiphase systems. For these purpose one has to establish equivalents of shift register, multiplier and modulo adder.

A direct method of generating pseudo-random phase shift sequences is to employ rf equivalents to the shift register element or the delay element, the modulo-p-adder and modulo-p-scalar multipliers, and interconnect them according to desired feedback logic. The shift register element would consist of a synchronised oscillator at a frequency of (either a n-phase oscillator or a subharmonic oscillator of order $1/n$) to which a gated rf input is applied (the duration of the gates (gating time) must be such as to ensure that the phase of the oscillator is locked to the phase of the input after the period of gating). The states or levels here correspond to the different possible phases (mod 2π). The mod—n adder would sum the phases of the inputs. For two inputs this is achieved by multiplying the two inputs.

The inputs and outputs of any element are capable of being at any time in any one of the n states represented by the digits 0, 1, 2, ..., $n-1$. The operations involved are synchronous *i.e* , the stored digits are forced to change at the same

time as in any clocked system. Ordinarily, the time separation between any two possible transitions is fixed signifying that the clock rate is fixed. There are however, situations when variable prf may be used with profit.

The behaviour of a given linear sequential network of the above type can be described in terms of the associated transfer matrix and the state diagram. The length of the cycle in a given network can be determined from the characteristic polynomial associated with the transfer marrix. One has to find the smallest integer k such that the characteristic polynomial divides X^k-1 without a remainder.

The block diagram of a shift register element is shown in figure 4. The input frequency is multiplied 4 times and this is mixed with a frequency which is thrice that of the input. The difference frequency is taken out after passing through a filter. The input is gated and fed to a synchronous oscillator which may be a subharmonic oscillator of order $1/n$ and can have n different phases. The phase of the sync. oscillator will be locked to that of the input phase if the input voltage is adequate, the switching time being dependent on input voltage and circuit Q. It is considered advisable to keep the circuit Q low during the period of switching and otherwise quite high.

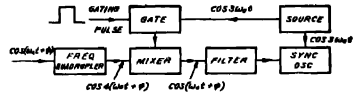

FIGURE 4. RF shift register for three phase system :—Unit phase shift for each circulation.

In multiphase systems multiplication means change of phase. Multiplication by 0 means that the component is absent, by 1 means it remains the same, by 2 means a phase change of $2\pi/n$, and so on. This can be incorporated only by extending the idea of shift register as shown in block diagram (figure 5).

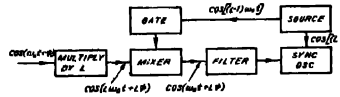

FIGURE 5. Phase multiplier :—Phase of the output L times the phase of the input.

The S-ary sequence is multiplied by $L = 2, 3, \ldots$ or n according to the requirement and mixed with a signal of frequency $(L-1)\ \omega t$. The difference frequency is selected and is fed to the sub-harmonic oscillator. The output of the oscillator will be in same phase as the input to it if the conditions discussed with shift-register are satisfied.

Another basic circuit of importance is the modulo addition circuit, block diagram of which is shown in figure 6. Here the product, of the two inputs cos $(\omega_0 t+\phi_1)$ and cos $(\omega_0+\phi_2)$ is taken and is mixed with a signal of frequency ω_0. The output signal phase will be equivalent to the signal whose phase is the sum of the two phases. As the phases are distributed in an equispaced closed field, the sum follows modular logic.

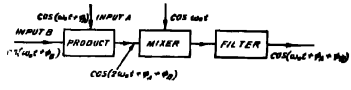

FIGURE 6. Phase adder (modulo) :— The output r f. carrier phase equivalent to the sum of the two input signal phases.

Now these basic blocks can be connected in the same fashion as stated earlier corresponding to the generating polynomial and we will obtain the desired sequence.

To generate polyphase codes discussed by Frank (1963), one can use the mod-p adder described above in combination with a shift-register in a feedback arrangement. For example if the code is 0,0,0,0; 0,1,2,3; 0,2,0,2; 0,3,2 1; one recognises that it is required to introduce phase advance per bit in the different blocks of length four of amount $\frac{n\,2\pi}{p}$ for the nth group. This can be achieved if one of the two inputs to mod-4 adder is obtained from a phase shift type ring counter, the other input being the output of the shift register.

The multi-phase output can, if desired, be modified into multilevel output by multiplying the multiphase voltage with a voltage having selected reference and passing the output through a low pass filter. For example in a ternary system if the phases of the outputs are 0°, 120°, 240°, then multiplication by a voltage at a reference phase of 90° will give outputs proportional to 0, 1, −1.

SECTION 3

Use of Multilevel Ternary PR Codes for Communication

Multilevel prs may be employed in any pulse digital modulation system by replacing the single pulse or state by the coded sequence. The additional unit required is a filter matched to the particular sequence.

PCM

In case of pulse code modulation the analog signal is first converted into a ternary code and then these ternary codes are used as the initial condition of the sequence generator. For analog digital conversion, two types of systems

which are in fact direct extensions of the concepts involving in binary Analog/ Digital converter have been found suitable.

In the first system analog signal is used to width modulate a pulse. The greater the amplitude of the sample of the analog signal larger is the width of the pulse. This width modulated pulse is now used to gate a train of clock pulses. Larger the width greater is the number of clock pulses allowed to pass. The number of clock pulses are counted in a ternary system.

The ternary counter is composed of a ring counter of order three. When the last stage of the ring counter is changing from 1 to 0 then only it can change the state of the following ring counter.

The block diagram of the system is shown in figure 7. If A_j of the system is ON then we will have a 'zero' in the position corresponding to the value of j.

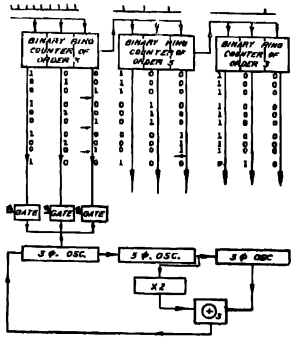

FIGURE 7. A ternary counter.

If B_j is ON we will have an 'one' in the position denoted by suffix j and if C_j is ON we will have a 'two' in the position of the suffix. As an example let us consider 19. Here looking into the ring counter we note that B_1 A_2 C_3 are ON, which can be represented by the ternary number 201. Now these initial conditions can be fed to the shift register generator.

In the other system we must have an idea of the amplitude of the signal. This gives us the knowledge about the digit of pulse the code consists of. For simplicity of discussion let us think that the maximum amplitude is less than 27.

The block diagram of the system is shown in figure 8. The input is first divided by 9 and this is fed to a three state device. The output of the three state device should correspond to the amplitude of the input both qualitatively

and quantitatively. The output is subtracted from the input of the three state device and it is divided by 9 and applied to another three state device. The

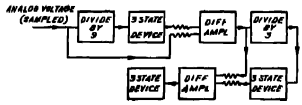

FIGURE 8. Alternative form of ternary counter.

same method is followed in the last stage also, and we get the state of the device as the code corresponding to the amplitude. This may similarly be used as an initial condition of the sequence generator If the maximum amplitude is more than 27 we have to increase the number of stages accordingly.

Binary ternary conversion

Since most present day data systems use binary mode, a binary to ternary converter would be very useful. At the moment the only technique available is to decode the binary/ternary code and then encode in ternary/binary code.

The decoding scheme is just as in binary. Here we have to select the weighted maximum and then add them up to get the amplitude back.

PPM

Ternary pr codes of length 13 are seen to have a high resolution in time. such codes are useful for ranging. To obtain PPM signal the analog signal is converted into quantised sample of amplitude and these are used to position modulate a series of pulses. The position modulated pulses can be used to trigger the prs generator. Thus the starting point of the sequence will now be proportional to the amplitude of the sample.

The function of the receiver is to decide from the correlator output about the starting time of the pulse.

M-ary

The sequences discussed earlier have little or no cross correlation if the integral is carried over the proper time period. In M-ary modulation one of the M alternative sequences is transmitted at a given time according to the data. The receiver compares the output of all M cross correlators and decides. The data signals in such cases are converted into PCM and the code is used as initial condition of the sequence generator. The receiver uses matched filter technique and finds out the maximum matched filter output by comparison.

Concluding Remarks

In this paper methods of generation of multilevel sequences both on amplitude and phase state basis have been presented. It has been shown that utilisation of phase logic results in considerable simplification in generation of phase-shift encoded multistate signals and their processing.

References

Briggs P. A. N. & Godfrey K. R. 1966, *Proc. I.E.E.*, **113**, 1259.
Church R. 1935, *Annals of Mathematics*, **36**, 198.
Elspas B. 1959, *IRE Trans. on Circuit Theory*.
Frank R. L. 1963, *IEEE Trans. on Information Theory*, IT-**9**, 43.
Golomb S. W. & Scholtz R. A. 1965, *IEEE Trans. on Information Theory*, IT-**11**, 533.
Pugh A. 1967. *Proc. I.E.E.*, **114**, 335.
Taub D. M. 1968, *Proc. I.E.E.*, **115**, 285.